CLAIMS

What is claimed is:

Sub a2

1. A method of authenticating a client, the method comprising:

receiving a record ID for a user, and a one-time key generated by the server and encrypted with a user's public key by the server;

receiving the user's authentication data from the client;

determining if the user's authentication data matches the record ID; and

if so, decrypting the one-time key with the user's private key, and returning the decrypted one-time key to the client.

2. The method of claim 1, further comprising registering the user, registering comprising:

receiving a registration authentication data from the user;

generating a random public key/private key pair for the user;

generating a random record ID for the user; and

associating the authentication data and the private key with the record ID.

3. The method of claim 2, further comprising:

sending the record ID and the public key to the user.

4. The method of claim 2, further comprising establishing a secure connection with the user, prior to receiving registration authentication data.

5. The method of claim 1, wherein a web page presented by the server to the client prompts the user to enter the authentication data to log in to the server.

6. The method of claim 5, wherein the client's authentication data is automatically redirected to the authentication server.

7. The method of claim 1, wherein the authentication data is biometric data.

8. The method of claim 1, wherein the authentication data is personal data selected from among the following: a password, a smart card, and another type of authentication card.

9. The method of claim 1, wherein the client forwards the decrypted one-time key to the server, thereby authenticating the user as the owner of the private key.

10. The method of claim 1, further comprising discarding the record ID after returning the one-time key to the user.

11. The method of claim 1, wherein the record ID and the encrypted one-time key are further encrypted using a partner key, the method further comprising decrypting the record ID and encrypted one-time key using the partner key.

12. The method of claim 11, wherein the partner key is a symmetric key set up during registration of the partner.

13. The method of claim 11, wherein the partner key is a private key of the authentication server.

14. A method of using a third party authentication server to authenticate a user to a server, the method comprising:

looking up a record ID associated with the user;

generating a one-time key and encrypting the one-time key with a public key of the user, and sending the encrypted one-time key and the record ID to the user;

receiving authentication data, the authentication data being the decrypted one-time key; and

permitting access to the server.

15. The method of claim 14, comprising:

determining an authentication policy associated with the user; and

verifying that the authentication policy has been satisfied, prior to permitting access to the server.

16. The method of claim 15, wherein verifying that the authentication policy has been satisfied comprises:

determining if the server should verify additional data; and

if so, requesting additional data from the user prior to generating the one-time key.

17. A third-party authentication system comprising:

an authentication server to receive a record ID for a user, and a one-time key generated by the server and encrypted with a user's public key by the server;

a comparison logic to receive user authentication data from the client and comparing whether the user's authentication data matches the record ID; and

a decryption logic to decrypt the one-time key with a private key associated with the validated record ID, and returning the decrypted one-time key to the client.

18. The system of claim 17, further comprising:

a policy validation logic to receive a policy from the server, and determine if the policy has been fulfilled; and

the decryption logic to decrypt the one-time key only if the policy has been fulfilled.

19. The system of claim 17, further comprising:

a nonce generation logic to generate a nonce, the nonce to be included with the user authentication data from the client; and

the comparison logic to verify that the user authentication data includes the appropriate nonce.

20. The system of claim 17, further comprising a client registration logic to register the user, the client registration logic comprising:

a key generation logic to generate a random public key/private key pair for the user;

a record ID generation logic to generate a random record ID for the user; and

the client registration logic to associate user authentication data with the private key and the record ID.

21. The system of claim 18, further comprising:

the interface to send the record ID and the public key to the user.

22. The system of claim 19, wherein the interface establish a secure connection with the user, prior to receiving registration authentication data.

23. The system of claim 17, wherein a web page presented by the server to the client prompts the user to enter the authentication data to log in to the server.

24. The system of claim 23, wherein the client's authentication data is automatically redirected to the authentication server.

25. The system of claim 17, wherein the authentication data is biometric data.

26. The system of claim 17, wherein the authentication data is personal data selected from among the following: a password, a smart card, and another type of authentication card.

27. The system of claim 17, wherein the client forwards the decrypted one-time key to the server, thereby authenticating the user as the owner of the private key.

28. The system of claim 17, further comprising a security mechanism to discard the record ID after returning the one-time key to the user.

29. The system of claim 17, wherein the decryption logic further decrypts the record ID and the encrypted one-time key with a partner key.

30. The system of claim 29, wherein the partner key is a symmetric key set up during registration of the partner.

31. The system of claim 29, wherein the partner key is a private key of the authentication server.